FICAM Testing Program Functional Requirements and Test Cases

VERSION 1.2.0

FIPS 201 EVALUATION PROGRAM

October 23, 2013

Office of Government wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	4/24/2013	Document creation	Limited
Draft	0.0.2	4/30/2013	Added background and objectives text, normative references	Limited
Draft	0.1.0	4/30/2013	Full comment resolution version for review	Limited
Draft	0.1.1	5/1/2013	Release candidate 1	Limited
Draft	0.1.2	5/2/2013	Revised per May 1, 2013 EPTWG Meeting	Limited
Draft	0.1.3	5/6/13	Draft Release	EPTWG
Draft	1.0.0 RC1	7/16/2013	Final review for program release	Limited
Draft	1.0.1 RC2	7/19/2013	QA updates approved	Limited
RC1	1.1.2	8/21/2013	Final release	Public
RC2	1.1.3	8/29/2013	Minor fixes	Limited
RC3	1.1.4	9/4/2013	CHUID deprecated; Credential # anti-collision specs added; Remove optional technologies	Limited
RC4	1.1.5	9/12/2013	Requirements for allowing PKI processing to be degraded and logging of failed certificates	Limited
RC5	1.1.6	9/20/2013	Improved credential processing; added 6 hour CRL requirement; added FICA< mode = no legacy; fixed path names; restored missing path tests 22-35; identified invalid test cases	Limited
Final	1.2.0	10/23/2013	Updated per initial testing for public release; used Reverse BCD format for 128-bit FASC-N; labeled incorrect tests for future update; identified test cases that will no longer be tested	Public

Table of Contents

1 Background

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) 201 Evaluation Program (EP) and its FIPS 201 Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance. GSA is currently transitioning the FIPS 201 EP and APL into the enhanced GSA FICAM Testing Program.

2 Change Control

This document will be updated in accord with the following schedule:

1. A new version will be published no less than six months from issuance of the current version. The new version is effective immediately.
2. If security or infrastructure risks are identified, an interim release may occur. Notice will be provided on effective dates for compliance to new requirements and test cases.

Notification of changes will be sent to the Evaluation Program Technical Working Group email list.

3 Objectives

This document identifies the functional requirements that the GSA FICAM Testing Program will perform on Physical Access Control Systems (PACS) submitted for evaluation. All requirements are instrumented using a smart card as presented to the system and various Public Key Infrastructure (PKI) paths. The PKI and smart cards test for specific common failures in cards and PKI, as well as Advanced Persistent Threat (APT) issues that impact PACS specifically. The PACS evaluation process is designed to be agnostic to architecture, and focuses solely on functional testing using an end-to-end testing methodology.

4 Test Instrumentation

The FICAM Testing Program for PACS relies on fully-defined, instrumented testing. This requires two core elements:

1. ***ICAM Test Cards*** – There are two cards that are completely valid and well formed. In addition, there are cards that have injected faults assuming both day-to-day operational errors as well as cards from a well-funded attacker.
2. ***Test PKI*** – This PKI provides the ability to link golden test cards with PKI faults. This provides the mechanism needed to verify that the system under test honors the PKI.

The full testing program, leveraging these test instruments, is described in *Appendix 1*.

4.1 ICAM Cards Used in Test

The following cards are used in the FICAM Testing Program.

1. Live PIV and PIV-I Cards from various issuers;
2. ICAM Test Cards (detailed in *Table 1*);
3. NIST PIV Test Cards; and
4. DoD JITC CAC Test Cards.

Table 1 - ICAM Test Cards Used in Test

ICAM Test Cards	Description	Threat Type
1	Golden PIV	None
2	Golden PIV-I	None
3	Substituted keypair in PKI-AUTH certificate	Manipulated Data
4	Tampered CHUID	Manipulated Data
5	Tampered PIV and Card Authentication Certificates	Manipulated Data
6	Tampered PHOTO	Manipulated Data
7	Tampered FINGERPRINT	Manipulated Data
8	Tampered SECURITY OBJECT	Manipulated Data
9	Expired CHUID signer	Invalid Date
10	Expired certificate signer	Invalid Date
11	PIV Authentication Certificate expiring after CHUID	Invalid Date
12	Authentication certificates valid in future	Invalid Date
13	Expired authentication certificates	Invalid Date
14	Expired CHUID	Invalid Date
15	Valid CHUID copied from one card to another **(PIV)**	Copied Credential
16	Valid Card Authentication Certificate copied from one card to another **(PIV)**	Copied Credential
17	Valid PHOTO copied from one card to another **(PIV)**	Copied Credential
18	Valid FINGERPRINT copied from one card to another **(PIV)**	Copied Credential
19	Valid CHUID copied from one card to another **(PIV-I)**	Copied Credential

ICAM Test Cards	Description	Threat Type
20	Valid Card Authentication Certificate copied from one card to another **(PIV-I)**	Copied Credential
21	Valid PHOTO copied from one card to another **(PIV-I)**	Copied Credential
22	Valid FINGERPRINT copied from one card to another **(PIV-I)**	Copied Credential
23	Private and Public Key mismatch	No Trusted Path
24	Revoked authentication certificates	Revoked Credential

4.2 PKI Used in Test

Table 2 describes the PKI infrastructure used for the FICAM Testing Program.

Table 2 - ICAM PKI path descriptions

Path Number	Fault description	Operational group
1	ICAM Invalid CA Signature	Manipulated Data
2	ICAM Invalid CA notBefore Date	Revoked/Date Invalid
3	ICAM Invalid CA notAfter Date	Revoked/Date Invalid
4	ICAM Invalid Name Chaining	Standards Conformant Processing
5	ICAM Missing Basic Constraints	Standards Conformant Processing
6	ICAM Invalid CA False Critical	Manipulated Data
7	ICAM Invalid CA False not Critical	Standards Conformant Processing
8	ICAM Invalid Path Length Constraint	Standards Conformant Processing
9	ICAM keyUsage keyCertSign False	Standards Conformant Processing
10	ICAM keyUsage Not Critical	Standards Conformant Processing
11	ICAM keyUsage Critical CRLSign False	Standards Conformant Processing
12	ICAM Invalid inhibitPolicyMapping	Standards Conformant Processing
13	ICAM Invalid DN nameConstraints	Standards Conformant Processing
14	ICAM Invalid SAN nameConstraints	Standards Conformant Processing
15	ICAM Invalid Missing CRL	Standards Conformant Processing
16	ICAM Invalid Revoked CA	Revoked/Date Invalid

Path Number	Fault description	Operational group
17	ICAM Invalid CRL Signature	Manipulated Data
18	ICAM Invalid CRL Issuer Name	Standards Conformant Processing
19	ICAM Invalid Old CRL nextUpdate	Revoked/Date Invalid
20	ICAM Invalid CRL notBefore	Revoked/Date Invalid
21	ICAM Invalid distributionPoint	Standards Conformant Processing
22	ICAM Valid requiredExplicitPolicy	Standards Conformant Processing
23	ICAM Invalid requiredExplicitPolicy	Standards Conformant Processing
24	ICAM Valid GeneralizedTime	PKI/Crypto Compatibility
25	ICAM Invalid GeneralizedTime	Standards Conformant Processing
26[1]	ICAM SHA-1 ECDSA prime256v1	PKI/Crypto Compatibility
27[2]	ICAM SHA-1 ECDSA secp384r1	PKI/Crypto Compatibility
28[3]	ICAM Invalid ECC Signature p256	Manipulated Data
29[4]	ICAM Invalid Policy Mapping p256	Standards Conformant Processing
30[5]	ICAM Invalid ECC Signature secp384r1	Manipulated Data
31[6]	ICAM Invalid Policy Mapping secp384r1	Standards Conformant Processing
32	ICAM Invalid SKID	Standards Conformant Processing
33	ICAM Invalid AKID	Standards Conformant Processing
34	ICAM Invalid CRL format	Standards Conformant Processing
35	ICAM 4096bit RSA key	PKI/Crypto Compatibility
36	ICAM Invalid CRL Signer	Standards Conformant Processing

[1] Invalid test. Uses SHA-1 not SHA-256.
[2] Invalid test. Uses SHA-1 not SHA-256.
[3] Invalid test. Uses SHA-1 not SHA-256.
[4] Invalid test. Uses SHA-1 not SHA-256.
[5] Invalid test. Uses SHA-1 not SHA-256.
[6] Invalid test. Uses SHA-1 not SHA-256.

6 Credential Number Processing

Table 3 describes the target state credential number processing rules. Target state requires all solutions to use 128-bit (16 byte) credential numbers to provide full protection against credential number collisions. These credential numbers shall be processed and stored in binary format. It is strongly recommended that credential numbers not be parsed into separate fields for interoperability, audit, and ease of testing purposes (see Test Cases 7.5.1, 7.5.2, and 7.8.3). If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes. The FICAM Testing Program anticipates new categories that have direct interaction with E-PACS (e.g., PSIM and PIAM). These new categories are anticipated to require that credential numbers be stored in a single field.

Systems that reduce credential numbers to less than 128-bits within any element of the E-PACS solution must provide compensating controls to avoid credential number collisions. In any case, credential numbers shall be greater than or equal to 64-bits. Such compensating controls will be deprecated on 10/21/2014.

Table 3 - Target State Credential Number Processing Rules

FASC-N Rule	
PIV and CAC: 128 Bit Output (Reverse BCD) FASC-N ID + CS + ICI + Pers Inden + Org Cat + Org Ind + Pers/Org (parity automatically removed)	Serial Output: 13 41 00 01 98 76 54 11 12 34 56 78 90 11 34 11
	Decoded Wiegand Data: 1 3 4 1 - 0 0 0 1 - 9 8 7 6 0001 0011 0100 0001-0000 0000 0000 0001-1001 1000 0111 0110 5 4 - 1 - 1 - 1 2 3 4 5 6 7 8 0101 0100-0001-0001-0001 0010 0011 0100 0101 0110 0111 1000 9 0 - 1 - 1 3 4 1 - 1 1001 0000-1000-1000 1100 0010 1000-1000
	Translated Card Data: Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1
UUID Rule	
PIV and PIV-I: 128 Bit UUID	16-byte binary representation of the UUID as defined by [RFC 4530].

Table 4 provides for the legacy/transitional state FASC-N credential number rules for PIV and CAC within the E-PACS. These formats will be deprecated by 10/21/2014.

Systems that use legacy/transitional state FASC-N credential number rules shall provide compensating controls to avoid credential number collisions. These controls shall achieve credential numbers that are greater than or equal to 64-bits.

Table 4 - Legacy/Transitional State FASC-N Credential Number Processing Rules

<table>
<tr><th colspan="2">Legacy/Transitional FASC-N Rules</th></tr>
<tr><td rowspan="3"><b><u>PIV:</u></b>
48 Bit Output (Each element individually formatted as binary numbers)
FASC-N ID</td><td><table><tr><th></th><th>Position</th><th>Length</th></tr><tr><td>Agency Code</td><td>1-14</td><td>14</td></tr><tr><td>System Code</td><td>15-28</td><td>14</td></tr><tr><td>Credential Number</td><td>29-48</td><td>20</td></tr></table></td></tr>
<tr><td>Binary Output:
10011010010-11011100101-10011111101111110001</td></tr>
<tr><td>Translated Card Data:
Agency Code = 1234, System Code = 1765, Credential Number = 654321</td></tr>
<tr><td rowspan="3"><b><u>CAC only:</u></b>
64 Bit Output (Reverse BCD)
FASC-N ID + CS and ICI
(parity automatically removed)</td><td>Serial Output:
13 41 00 01 98 76 54 11</td></tr>
<tr><td>Decoded Wiegand Data:
1 3 4 1 - 0 0 0 1 - 9 8 7 6
0001 0011 0100 0001-0000 0000 0000 0001-1001 1000 0111 0110
5 4 - 1 - 1
0101 0100-0001-0001</td></tr>
<tr><td>Translated Card Data:
Agency Code = 1341, System Code = 0001, Credential Number = 987654, Credential Series = 1, Issue Code = 1</td></tr>
<tr><td rowspan="2"><b><u>PIV and CAC:</u></b>
200 Bit Output</td><td>Serial Output:
D4 32 48 58 21 0C 2D 31 71 B5 25 A1 68 5A 08 C9 2A DE 0A 61 84 32 48 43 E2</td></tr>
<tr><td>Decoded Wiegand Data:</td></tr>
</table>

(BCD) Full FASC-N	SS 1 3 4 1 D 0 0 0 1101 0 1000 0 1100 1 0010 0 1000 0 1011 0 0000 1 0000 1 0000 1 D 9 8 7 6 5 4 1 1000 0 1011 0 1001 1 0001 0 1110 0 0110 1 1010 1 0010 D 1 D 1 D 1 2 3 0 1011 0 1000 0 1011 0 1000 0 1011 0 1000 0 0100 0 1100 4 5 6 7 8 9 0 1 1 0010 0 1010 1 0110 1 1110 0 0001 0 1001 1 0000 1 1000 1 3 4 1 1 F 8 0 1000 0 1100 1 0010 0 1000 0 1000 0 1111 1 0001 0
	Translated Card Data: Agency Code = 1341, System Code: 0001, Credential Number: 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1, LRC = 8

7 Normative References

[HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004
https://www.dhs.gov/homeland-security-presidential-directive-12

[FIPS 201] Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[Common] FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.17, December 9, 2011
http://idmanagement.gov/documents/federal-pki-common-policy-framework-certificate-authority

[FBCA] FBCA X.509 Certificate Policy For Federal Bridge Certification Authority (FBCA), Version 2.25, December 9, 2011
http://idmanagement.gov/fbca-certificate-policy-page

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), DRAFT Version 2.0.2, May 24, 2012

[M-05-24] Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf

[M-06-18] Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf

[M-11-11] OMB Memorandum M-11-11, February 3, 2011
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
http://idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance

[SP800-116] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008
http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

[SP800-73] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-3, Parts 1-3, February 2010
http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART2_piv-card-applic-card-common-interface.pdf

http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART3_piv-client-applic-programming-interface.pdf

[SP800-76] NIST SP 800-76-1, January 2007
http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

[SP800-78] NIST SP 800-78-3, December 2010
http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf

[SP800-96] NIST SP 800-96, September 2006
http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[RFC 4530] IETF RFC 4530, “Lightweight Directory Access Protocol (LDAP) entry UUID Operational Attribute,” June 2006
http://www.ietf.org/rfc/rfc4530.txt

[UL 294] The Standard of Safety for Access Control System Units, UL Edition Number – 5, Date 01/29/1999, Type ULSTD
http://www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

[UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number – 5, Date 09/29/1995, Type ULSTD
http://www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

[UL 1981] The Standard for Central-Station Automation Systems UL Edition Number -2, Date 06/30/2003, Type ULSTD
http://www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

Appendix 1 Functional Requirements and Test Cases

1.	Scoring Guidelines
	Security - A control directly impacting security of the system.
	Usability - A control impacting end user system usability. Does not directly impact security.
	Required - Must be present. Must work correctly: Red/Green.
	Optional - May be present. If present, it must work correctly: Red/Green. Not present: Yellow.

Products to be listed on the APL shall not have any tests scored RED. Products listed on the APL may have tests scored YELLOW.

			2.	Requirements at Time of In-Person Registration In Accordance With [E-PACS] PIA-9	*All tests use PKI-AUTH unless specifically noted.* *All tests using a CONTACT reader unless specifically noted.*	*Note all requirements sourced from [E-PACS] unless otherwise noted.*
Security/ Usability	**Required/ Optional**	**Test #**	**Test**	**Requirement**	**Test Case: Pass/Fail criteria**	**Requirement Source**
			2.1.	**Signature Verification**		
Security	Required	1	2.1.1.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential	Card 1: PIV Golden Registers successfully.	PIA-2 thru PIA-7
Security	Required	2	2.1.2.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Card 2: PIV-I Golden Registers successfully	PIA-2 thru PIA-7
Security	Required	3	2.1.3.	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path	Card 1: (Golden PIV Card) w/PKI Path 1 fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4, PIA-5
Security	Required	4	2.1.4.	Verify product's ability to recognize invalid signature on the End Entity certificate	Card 5: invalid PIV/Card Auth Signer fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4

Security	Required	5	2.1.5.	Verify product’s ability to recognize certificate/private key mismatch	Card 23: Certificate Private Key mismatch fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
			2.2.	**Certificate Validity Periods**		
Security	Required	6	2.2.1.	Verify product’s ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future	Card 1: (Golden PIV Card) w/PKI Path 2 fails to register successfully.	PIA-3.5, PIA-5
Security	Required	7	2.2.2.	Verify product’s ability to reject a credential when notAfterDate of the End Entity Signing CA is sometime in the past.	Card 10: expired signing CA fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
Security	Required	8	2.2.3.	Verify product’s ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future	Card 12: (Certs not yet valid) fails to register successfully.	PIA-3.5
Security	Required	9	2.2.4.	Verify product’s ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past	Card 1: (Golden PIV Card) w/PKI Path 3 fails to register successfully.	PIA-3.5, PIA-5
Security	Required	10	2.2.5.	Verify product’s ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past	Card 13: (Certs Expired) fails to register successfully.	PIA-3.5
			2.3.	**Name Chaining**		

Security	Required	11	2.3.1.	Verify product’s ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate	Card 1: (Golden PIV Card) w/PKI Path 4 fails to register successfully.	PIA-3.2, PIA-5
			2.4.	**Basic Constraints Verification**		
Security	Required	12	2.4.1.	Verify product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Card 1: (Golden PIV Card) w/PKI Path 5 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	13	2.4.2.	Verify product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) w/PKI Path 6 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	14	2.4.3.	Verify product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) w/PKI Path 7 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	15	2.4.4.	Verify product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second	Card 1: (Golden PIV Card) w/PKI Path 8 fails to register successfully.	PIA-3.2, PIA-5

				intermediate CA certificate and an End Entity certificate.		
Security	Required	16	2.4.5.	Verify product’s ability to detect a mismatched SKID with the subject public key in the certificate.	Card 1: (Golden PIV Card) w/PKI Path 32 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	17	2.4.6.	Verify product’s ability to detect a mismatched AKID with the authority (issuer) public key in the certificate.	Card 1: (Golden PIV Card) w/PKI Path 33 fails to register successfully.	PIA-3.2, PIA-5
			2.5.	**Key Usage Verification**		
Security	Required	18	2.5.1.	Verify product’s ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false	Card 1: (Golden PIV Card) w/PKI Path 9 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	19	2.5.2.	Verify product’s ability to recognize when the intermediate certificate includes a non-critical keyUsage extension	Card 1: (Golden PIV Card) w/PKI Path 10 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	20	2.5.3.	Verify product’s ability to recognize when the intermediate certificate includes a critical keyUsage extension in which crlSign is false	Card 1: (Golden PIV Card) w/PKI Path 11 fails to register successfully.	PIA-3.2, PIA-5
			2.6.	**Certificate Policies**		

Security	Required	21	2.6.1.	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware.	Production PIV registers successfully	PIA-3.2, PIA-5
Security	Required	22	2.6.2.	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).	Production PIV fails to register	PIA-3.2, PIA-5
Security	Required	23	2.6.3.	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware. Test Condition: production PIV passes	Production PIV registers successfully	PIA-3.2, PIA-5

Security	Required	24	2.6.4.	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4).	Production PIV fails to register	PIA-3.2, PIA-5
Security	Required	25	2.6.5.	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (ex, High Hardware).	Production PIV fails to register	PIA-3.2, PIA-5
Security	Required	26	2.6.6.	With no policy set, verify product's ability to process requiredExplicitPolicy.	Card 1: (Golden PIV Card) w/PKI Path 22 fails to register successfully.	PIA-3.2, PIA-5

Security	Required	27	2.6.7.	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path with an invalid setting for requiredExplicitPolicy.	Card 1: (Golden PIV Card) w/PKI Path 23 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	28	2.6.8.	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B	Card 1: (Golden PIV Card) w/PKI Path 12 fails to register successfully.	PIA-3.2, PIA-5
			2.7.	**Generalized Time**		
Security	Required	29	2.7.1.	Verify product's ability to process valid use of generalized time post year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 24 registers successfully.	PIA-3.2, PIA-5
Security	Required	30	2.7.2.	Verify product's ability to process invalid use of generalized time before year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 25 fails to register successfully.	PIA-3.2, PIA-5
			2.8.	**Name Constraints**		

Security	Required	31	2.8.1.	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) registers successfully.	PIA-3.2, PIA-5
Security	Required	32	2.8.2.	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) w/PKI Path 13 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	33	2.8.3.	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-5
			2.9.	**Certificate Revocation Tests (CRL)**		
Security	Required	34	2.9.1.	The system recognizes when no revocation information is available for the End Entity certificate	Card 1: (Golden PIV Card) w/PKI Path 15 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	35	2.9.2.	The system recognizes when a second intermediate CA certificate is revoked	Card 1: (Golden PIV Card) w/PKI Path 16 fails to register	PIA-3.5, PIA-5,

					successfully.	PIA-7
Security	Required	36	2.9.3.	The system recognizes when the End Entity certificate is revoked	Card 24: (Revoked status) fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	37	2.9.4.	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert	Card 1: (Golden PIV Card) w/PKI Path 18 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	38	2.9.5.	The system recognizes when a certificate in the path points to a CRL with an expired nextUpdate value (an expired CRL)	Card 1: (Golden PIV Card) w/PKI Path 19 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	39	2.9.6.	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	Card 1: (Golden PIV Card) w/PKI Path 20 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	40	2.9.7.	The system recognizes when a certificate in the path has an incorrect CRL distribution point	Card 1: (Golden PIV Card) w/PKI Path 21 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	41	2.9.8.	The system recognizes when the CRL has an invalid signature	Card 1: (Golden PIV Card) w/PKI Path 17 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	42	2.9.9.	The system recognizes when an incorrectly formatted CRL is present in the path.	Card 1: (Golden PIV Card) w/PKI Path 34 fails to register successfully.	PIA-3.5, PIA-5, PIA-7

Security	Required	43	2.9.10.	The system recognizes when an invalid CRL signer is in the path.	Card 1: (Golden PIV Card) w/PKI Path 36 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
			2.10.	**CHUID Verification**		
Security	Required	44	2.10.1.	The system recognizes when the CHUID signature is invalid and does not verify	Card 4: (Invalid CHUID Signature) fails to register successfully.	PIA-3.2, PIA-4
Security	Required	45	2.10.2.	The system recognizes when the CHUID signer certificate is expired	Card 9: (Expired CHUID signer) fails to register successfully.	PIA-3.6, PIA-5
Security	Required	46	2.10.3.	The system recognizes when the CHUID is expired	Card 14: (Card Expired) fails to register successfully	PIA-3.6
Security	Required	47	2.10.4.	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert	Card 15: (FASC-N in CHUID !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	48	2.10.5.	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I Auth Cert	Card 19: (UUID in CHUID !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.3
Security	Required	49	2.10.6.	The system recognizes when the PKI-AUTH certificate expires after the CHUID expiration date.	Card 11: (PKI-AUTH Cert after CHUID) fails to register successfully	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
			2.11.	**Facial Image Verification**	If Facial Image is Supported, tests in this section are Required.	

Security	Required	50	2.11.1.	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails to register successfully	PIA-3.2, PIA-4
			2.12.	**Copied Containers**		
Security	Required	51	2.12.1.	The system recognizes when the FASC-N in the PKI-CAK certificate does not equal the FASC-N in the PIV Auth Cert	Card 16: (FASC-N in PKI-CAK Cert !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	52	2.12.2.	The system recognizes when the UUID in the PKI-CAK certificate does not equal the UUID in the PIV-I Auth Cert	Card 20: (UUID in PKI-CAK Cert !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	53	2.12.3.	The system recognizes when the FASC-N in the Facial Image does not equal the FASC-N in the PIV Auth Cert	Card 17: (FASC-N in Facial Image !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	54	2.12.4.	The system recognizes when the UUID in the Facial Image does not equal the UUID in the PIV-I Auth Cert	Card 21: (UUID in Facial Image !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
			2.13.	**FINGERPRINT Verification**	If BIO Auth Meth is Supported at time of registration, tests in this section are Required. If content signer certificate is from CHUID, Section 2.10 is Required.	
Security	Required	55	2.13.1.	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Card 7: (bad fingerprint signature) fails to register successfully	PIA-3.2, PIA-4

Security	Required	56	2.13.2.	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5
Security	Required	57	2.13.3.	Verify Product's ability to accept a valid credential with a matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented correct bearer's fingerprint. Registration succeeds.	PIA-3 thru PIA-7
Security	Required	58	2.13.4.	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented incorrect bearer's fingerprint. Registration fails.	PIA-3.3
Security	Required	59	2.13.5.	The system recognizes when the FASC-N in the Fingerprint does not equal the FASC-N in the PIV Auth Cert	Card 18: (FASC-N in Fingerprint !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	60	2.13.6.	The system recognizes when the UUID in the Fingerprint does not equal the UUID in the PIV-I Auth Cert	Card 22: (UUID in Fingerprint !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
			2.14.	**Security Object Verification**	If Security Object is Supported, tests in this section are Required.	

Security	Required	61	2.14.1.	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) fails to register successfully	PIA-3.4, PIA-4, PIA-5
			2.15.	**OCSP Response Checking**		
Security	Required	62	2.15.1.	The system successfully validates a good credential using an OCSP response with a good signature	Card 1: Golden PIV registers successfully	PIA-3.2, PIA-3.5
Security	Required	63	2.15.2.	Validation fails using an OCSP Responder with an expired signature certificate for a good card.	Card 1: Golden PIV fails to register successfully	PIA-3.2 PIA-3.5, PIA-3.6
Security	Required	64	2.15.3.	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV registers successfully	PIA-3.2, PIA-3.5
Security	Required	65	2.15.4.	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV fails to register successfully	PIA-3.2, PIA-3.5, PIA-3.6
Security	Required	66	2.15.5.	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.	Card 1: Golden PIV fails to register successfully	PIA-3.2, PIA-4
			2.16.	**Interoperability Testing**	Tests in this section attempt to use a variety of dual interface and dual chip production PIV and PIV-I	

					cards in the system.	
Usability	Required	67	2.16.1.	Various valid PIV (including CAC) and PIV-I cards can be individually registered using PKI-AUTH method.	PIV (including CAC) and PIV-I cards register successfully	PIA-6
			2.17.	**Cryptography Testing**		
Security	Required	68	2.17.1.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	NIST card#7 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	69	2.17.2.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	70	2.17.3.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

					available.	
Security	Optional	71	2.17.4.	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	(valid through 1/1/2014) Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	72	2.17.5.	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	73	2.17.6.	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

					available.	
Security	Required	74	2.17.7.	Verify Product’s ability to validate signatures using ECDSA (P-256)	NIST card#4 registers successfully. (Replaces ICAM Path 26)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	75	2.17.8.	Verify Product’s ability to validate signatures using ECDSA (P-384)	NIST card#5 registers successfully. (Replaces ICAM Path 27)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	76	2.17.9.	Verify Product’s ability to validate signatures using SHA-1	NIST card#7 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Required	77	2.17.10.	Verify Product’s ability to validate signatures using SHA-256	NIST card#1 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Optional	78	2.17.11.	Verify Product’s ability to validate signatures using SHA-384	NIST card#5 registers successfully.	[SP800-78] Table 3-7; [Common]

						§6.1.5
Security	Required	79	2.17.12.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	NIST card#1 registers successfully.	[SP800-78] Table 3-2
Security	Optional	80	2.17.13.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 2^256-1.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-2
Security	Required	81	2.17.14.	Verify product's ability to validate signatures using RSA 4096 in the path.	Card 1: (Golden PIV Card) w/PKI Path 35 registers successfully	
			2.18.	**PIN Testing**		
Security	Required	82	2.18.1.	Verify Application and Global PINs and their corresponding failed attempt counters operate in accord with the Discovery Object.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-73] Part 1, §3.2.6

			3.	Dual Chip Card, time of registration	Requirements for Dual Chip Cards will not be tested prior to June 1, 2014. These requirements become mandatory as of June 1, 2014. Products certified prior to June 1, 2014 shall come into conformance within six months from the date the test cards and PKI are made available for dual chip testing.	[FIPS 201]
			3.1.	**CHUID Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader**	
Security	Required	83	3.1.1.	The system recognizes when the CHUID signature is invalid and does not verify	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2, PIA-4
Security	Required	84	3.1.2.	The system recognizes when the CHUID signer certificate is expired	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance	PIA-3.6, PIA-5

					within six months from the date the test cards and PKI are made available.	
Security	Required	85	3.1.3.	The system recognizes when the CHUID is expired	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.6
Security	Required	86	3.1.4.	The system recognizes when the PKI-CAK certificate expires after the CHUID expiration date.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
			3.2.	**Copied Containers**		
Security	Required	87	3.2.1.	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV PKI-CAK Cert	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance	PIA-3.2; [SP800-73], Part 1, §3.1.2

					within six months from the date the test cards and PKI are made available.	
Security	Required	88	3.2.2.	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I PKI-CAK Cert	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.2; [SP800-73], Part 1, §3.1.2
			3.3.	**Signature Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader. PKI-CAK mode is used for all tests.**	
Security	Required	89	3.3.1.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2 thru PIA-7
Security	Required	90	3.3.2.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to	PIA-2 thru PIA-7

					availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	
Security	Required	91	3.3.3.	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4, PIA-5
Security	Required	92	3.3.4.	Verify product's ability to recognize invalid signature on the End Entity certificate	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4
Security	Required	93	3.3.5.	Verify product's ability to recognize certificate/private key mismatch	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance	PAI-3.2, PIA-3.4, PIA-4

					within six months from the date the test cards and PKI are made available.	
			4.	**Requirements for Automated Provisioning In Accordance With [E-PACS] PIA-8**	.	
			4.1.	**Dual Interface Chip Card**		
Security	Optional	94	4.1.1.	The E-PACS shall accept automated provisioning from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	Perform design analysis of automated provisioning functionality of the solution.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94
Security	Optional	95	4.1.2.	The E-PACS shall accept automated deprovisioning from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	Perform design analysis of automated deprovisioning functionality of the solution.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94
			4.2.	**Dual Chip Card**	Requirements for Dual Chip Cards will not be tested prior to June 1, 2014. These requirements become mandatory as of June 1, 2014.	[FIPS 201]

					Products certified prior to June 1, 2014 shall come into conformance within six months from the date the test cards and PKI are made available for dual chip testing.	
Security	Optional	96	4.2.1.	The E-PACS shall accept automated provisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	Perform design analysis of automated provisioning functionality of the solution.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94
Security	Optional	97	4.2.2.	The E-PACS shall accept automated deprovisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	Perform design analysis of automated deprovisioning functionality of the solution.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94
			5.	**Authentication at Time of Access Test Cases**	All tests use PKI-AUTH unless specifically noted.	
			5.1.	**Signature Verification**		
Security	Required	98	5.1.1.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential	Card 1: PIV Golden Receives an access grant Successfully	PIA-2 thru PIA-7

Security	Optional	99	5.1.2.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Card 2: PIV-I Golden Receives an access grant Successfully	PIA-2 thru PIA-7
Security	Required	100	5.1.3.	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path	Card 1: (Golden PIV Card) w/PKI Path 1 fails to receive an access grant	PAI-3.2, PIA-3.4, PIA-4, PIA-5
Security	Required	101	5.1.4.	Verify product's ability to recognize invalid signature on the End Entity certificate	Card 5: invalid PIV/Card Auth Signer fails to receive an access grant	PAI-3.2, PIA-3.4, PIA-4
Security	Required	102	5.1.5.	Verify product's ability to recognize certificate/private key mismatch	Card 23: Certificate Private Key mismatch fails to receive an access grant.	PAI-3.2, PIA-3.4, PIA-4
Security	Required	103	5.1.6.	Verify product's ability to recognize public key from card does not match public key previously registered to the system.	Card 3: Substituted keypair in PKI-AUTH certificate fails to receive an access grant.	PIA-3.2
			5.2.	**Certificate Validity Periods**		
Security	Required	104	5.2.1.	Verify product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future	Card 1: (Golden PIV Card) fails access grant w/PKI Path 2	PIA-3.5, PIA-5
Security	Required	105	5.2.2.	Verify product's ability to reject a credential when notBefore date of the End Entity certificate is sometime in the	Card 12: (Certs not yet valid) access grant fails	PIA-3.5

				future		
Security	Required	106	5.2.3.	Verify product’s ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past	Card 1: (Golden PIV Card) fails access grant w/PKI Path 3	PIA-3.5, PIA-5
Security	Required	107	5.2.4.	Verify product’s ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past	Card 13: (Certs Expired) access grant fails	PIA-3.5
			5.3.	**Name Chaining**		
Security	Required	108	5.3.1.	Verify product’s' ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate	Card 1: (Golden PIV Card) fails access grant w/PKI Path 4	PIA-3.2, PIA-5
			5.4.	**Basic Constraints Verification**		
Security	Required	109	5.4.1.	Verify product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 5	PIA-3.2, PIA-5
Security	Required	110	5.4.2.	Verify product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) fails access grant w/PKI Path 6	PIA-3.2, PIA-5

Security	Required	111	5.4.3.	Verify product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) fails access grant w/PKI Path 7	PIA-3.2, PIA-5
Security	Required	112	5.4.4.	Verify product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 8	PIA-3.2, PIA-5
Security	Required	113	5.4.5.	Verify product’s ability to detect a mismatched SKID with the subject public key in the certificate.	Card 1: (Golden PIV Card) w/PKI Path 32 receives access denied.	PIA-3.2, PIA-5
Security	Required	114	5.4.6.	Verify product’s ability to detect a mismatched AKID with the authority (issuer) public key in the certificate.	Card 1: (Golden PIV Card) w/PKI Path 33 receives access denied.	PIA-3.2, PIA-5

			5.5.	**Key Usage Verification**		
Security	Required	115	5.5.1.	Verify product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false	Card 1: (Golden PIV Card) fails access grant w/PKI Path 9	PIA-3.2, PIA-5
Security	Required	116	5.5.2.	Verify product's ability to recognize when the intermediate certificate includes a non-critical keyUsage extension	Card 1: (Golden PIV Card) fails access grant w/PKI Path 10	PIA-3.2, PIA-5
Security	Required	117	5.5.3.	Verify product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which crlSign is false	Card 1: (Golden PIV Card) fails access grant w/PKI Path 11	PIA-3.2, PIA-5
			5.6.	**Certificate Policies**		
Security	Required	118	5.6.1.	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware.	Production PIV receives access grant	PIA-3.2, PIA-5

Security	Required	119	5.6.2.	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).	Production PIV receives access denied	PIA-3.2, PIA-5
Security	Required	120	5.6.3.	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware. Test Condition: production PIV passes	Production PIV receives access grant	PIA-3.2, PIA-5
Security	Required	121	5.6.4.	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4).	Production PIV receives access denied	PIA-3.2, PIA-5

Security	Required	122	5.6.5.	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (ex, High Hardware).	Production PIV receives access denied	PIA-3.2, PIA-5
Security	Required	123	5.6.6.	With no policy set, verify product's ability to process requiredExplicitPolicy.	Card 1: (Golden PIV Card) w/PKI Path 22 receives access denied.	PIA-3.2, PIA-5
Security	Required	124	5.6.7.	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path with an invalid setting for requiredExplicitPolicy.	Card 1: (Golden PIV Card) w/PKI Path 23 receives access denied.	PIA-3.2, PIA-5
Security	Required	125	5.6.8.	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B	Card 1: (Golden PIV Card) fails access grant w/PKI Path 12	PIA-3.2, PIA-5

			5.7.	**Generalized Time**		
Security	Required	126	5.7.1.	Verify product's ability to process valid use of generalized time post year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 24 receives access grant.	PIA-3.2, PIA-5
Security	Required	127	5.7.2.	Verify product's ability to process invalid use of generalized time before year 2049 in the path.	Card 1: (Golden PIV Card) w/PKI Path 25 denied access.	PIA-3.2, PIA-5
			5.8.	**Name Constraints**		
Security	Required	128	5.8.1.	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) access grant succeeds	PIA-3.2, PIA-5
Security	Required	129	5.8.2.	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 13	PIA-3.2, PIA-5
Security	Required	130	5.8.3.	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance	PIA-3.2, PIA-5

				subjectAltName with a DN that falls outside that subtree.	within six months from the date the test cards and PKI are made available.	
			5.9.	**Certificate Revocation Tests (CRL)**		
Security	Required	131	5.9.1.	The system recognizes when no revocation information is available for the End Entity certificate	Card 1: (Golden PIV Card) fails access grant w/PKI Path 15	PIA-3.5, PIA-5, PIA-7
Security	Required	132	5.9.2.	The system recognizes when a second intermediate CA certificate is revoked	Card 1: (Golden PIV Card) fails access grant w/PKI Path 16	PIA-3.5, PIA-5, PIA-7
Security	Required	133	5.9.3.	The system recognizes when the End Entity certificate is revoked	No longer tested. Chasing CDP from the certificate on the card at time of access should never happen. CDP should only be trusted based on registration process. Card 24: Revoked status	PIA-3.5, PIA-5, PIA-7
Security	Required	134	5.9.4.	The system recognizes when the CRL has an invalid signature	Card 1: (Golden PIV Card) fails access grant w/PKI Path 17	PIA-3.5, PIA-5, PIA-7
Security	Required	135	5.9.5.	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which	Card 1: (Golden PIV Card) fails access grant w/PKI Path 18	PIA-3.5, PIA-5, PIA-7

				issued the cert		
Security	Required	136	5.9.6.	The system recognizes when a certificate in the path has an expired nextUpdate value (an expired CRL)	Card 1: (Golden PIV Card) fails access grant w/PKI Path 19	PIA-3.5, PIA-5, PIA-7
Security	Required	137	5.9.7.	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	Card 1: (Golden PIV Card) fails access grant w/PKI Path 20	PIA-3.5, PIA-5, PIA-7
Security	Required	138	5.9.8.	The system recognizes when a certificate in the path has an incorrect CRL distribution point	Card 1: (Golden PIV Card) fails access grant w/PKI Path 21	PIA-3.5, PIA-5, PIA-7
Security	Required	139	5.9.9.	The system recognizes when an incorrectly formatted CRL is present in the path.	No longer tested. Chasing CDP from the certificate on the card at time of access should never happen. CDP should only be trusted based on registration process. Card 1: (Golden PIV Card) fails access grant w/PKI Path 34	PIA-3.5, PIA-5, PIA-7
Security	Required	140	5.9.10.	The system recognizes when an invalid CRL signer is in the path.	No longer tested. Chasing CDP from the certificate on the card at time of access should never happen. CDP should only be trusted based on registration process. Card 1: (Golden PIV Card) fails	PIA-3.5, PIA-5, PIA-7

					access grant w/PKI Path 36	
			5.10.	**CHUID Verification**	The CHUID Authentication Method is **DEPRECATED**.	
			5.11.	**Facial Image Verification**	If showing facial image as part of an access transaction is Supported, tests in this section are Required.	
Security	Required	141	5.11.1.	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails access grant	PIA-3, PIA-3.2, PIA-3.3, PIA-4
			5.12.	**FINGERPRINT Verification**	If BIO Auth Meth is Supported, tests in this section are Required.	
Security	Required	142	5.12.1.	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Card 7: (bad fingerprint signature) access grant fails	PIA-3, PIA-3.2, PIA-3.3, PIA-4
Security	Required	143	5.12.2.	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5

					the test cards and PKI are made available.	
Security	Required	144	5.12.3.	Verify Product's ability to accept a valid credential with a matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented correct bearer's fingerprint. Access is granted.	PIA-3 thru PIA-7
Security	Required	145	5.12.4.	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented incorrect bearer's fingerprint. Access grant fails.	PIA-3.3
			5.13.	**Security Object Verification**	If Security Object is Supported, tests in this section are Required.	
Security	Required	146	5.13.1.	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) access grant fails	PIA-3.4, PIA-4, PIA-5
			5.14.	**OCSP Response Checking**		
Security	Required	147	5.14.1.	The system successfully validates a good credential using an OCSP response with a good signature	Card 1: Golden PIV is granted access	PIA-3.2, PIA-3.5
Security	Required	148	5.14.2.	Validation fails using an OCSP Responder with an expired signature certificate for a good card.	Card 1: Golden PIV access is denied	PIA-3.2 PIA-3.5, PIA-3.6

Security	Required	149	5.14.3.	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV is granted access	PIA-3.2, PIA-3.5
Security	Required	150	5.14.4.	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV access is denied	PIA-3.2, PIA-3.5, PIA-3.6
Security	Required	151	5.14.5.	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.	Card 1: Golden PIV access is denied	PIA-3.2, PIA-4
			5.15.	**Interoperability Testing**	Tests in this section attempt to use a variety of dual interface production PIV and PIV-I cards in the system.	
Usability	Required	152	5.15.1.	Various valid PIV (including CAC) and PIV-I cards are granted access using PKI-AUTH method.	PIV (including CAC) and PIV-I cards are granted access	PIA-6
			5.16.	**Cryptography testing**		
Security	Required	153	5.16.1.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	NIST card#7 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

Security	Required	154	5.16.2.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 is granted access.	[SP800-78] Table 3-1;
						[SP800-78] Table 3-3;
						[Common] §6.1.5

Security	Required	155	5.16.3.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-1;
						[SP800-78] Table 3-3;
						[Common] §6.1.5

Security	Optional	156	5.16.4.	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	(valid through 1/1/2014)
					Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.
						[SP800-78] Table 3-1;
						[SP800-78] Table 3-3;
						[Common] §6.1.5

Security	Optional	157	5.16.5.	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	158	5.16.6.	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	159	5.16.7.	Verify Product’s ability to validate signatures using ECDSA (P-256)	NIST card#4 is granted access. (Replaces ICAM Path 26)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	160	5.16.8.	Verify Product’s ability to validate signatures using ECDSA (P-384)	NIST card#5 is granted access. (Replaces ICAM Path 27)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

Security	Optional	161	5.16.9.	Verify Product's ability to validate signatures using SHA-1	NIST card#7 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Required	162	5.16.10.	Verify Product's ability to validate signatures using SHA-256	NIST card#1 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Optional	163	5.16.11.	Verify Product's ability to validate signatures using SHA-384	NIST card#5 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Required	164	5.16.12.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	NIST card#1 is granted access.	[SP800-78] Table 3-2
Security	Optional	165	5.16.13.	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 2^256-1.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-78] Table 3-2
Security	Required	166	5.16.14.	Verify product's ability to validate signatures using RSA 4096 in the path.	Card 1: (Golden PIV Card) w/PKI Path 35 is granted access.	

			5.17.	**PIN Testing**		
Security	Required	167	5.17.1.	Verify Application and Global PINs and their corresponding failed attempt counters operate in accord with the Discovery Object.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	[SP800-73] Part 1, §3.2.6
			6.	**Dual Chip Card, time of access**	Requirements for Dual Chip Cards will not be tested prior to June 1, 2014. These requirements become mandatory as of June 1, 2014. Products certified prior to June 1, 2014 shall come into conformance within six months from the date the test cards and PKI are made available for dual chip testing.	[FIPS 201]
			6.1.	**CHUID Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader**	
Security	Required	168	6.1.1.	The system recognizes when the CHUID signature is invalid and does not verify	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI	PIA-3.2, PIA-4

					shall come into conformance within six months from the date the test cards and PKI are made available.	
Security	Required	169	6.1.2.	The system recognizes when the CHUID signer certificate is expired	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.6, PIA-5
Security	Required	170	6.1.3.	The system recognizes when the CHUID is expired	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-3.6
			6.2.	**Signature Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader. PKI-CAK mode is used for all tests.**	
Security	Required	171	6.2.1.	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV credential	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI.	PIA-2 thru PIA-7

					Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	
Security	Required	172	6.2.2.	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PIA-2 thru PIA-7
Security	Required	173	6.2.3.	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4, PIA-5
Security	Required	174	6.2.4.	Verify product's ability to recognize invalid signature on the End Entity certificate	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI	PAI-3.2, PIA-3.4, PIA-4

					shall come into conformance within six months from the date the test cards and PKI are made available.	
Security	Required	175	6.2.5.	Verify product’s ability to recognize certificate/private key mismatch	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PAI-3.2, PIA-3.4, PIA-4
			7.	**PACS Design Use Cases**		
			7.1.	**Continuity of Operations Testing**		
Usability	Optional	176	7.1.1.	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	For each component within a solution, disconnect the network to the component. Using Test Card 1: Golden, document success/failure.	PCP-1

Usability	Optional	177	7.1.2.	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	For each service within a solution, manually stop the service on the server(s). Test Card 1: PIV Golden, document success/failure.	PCP-1
Usability	Optional	178	7.1.3.	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for a valid credential.	For each component within the solution, abruptly remove all power sources from the power supply. Restore power. Attempt access with Test Card 1: PIV Golden, document success/failure.	PCP-1
Usability	Optional	179	7.1.4.	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PCP-1
Usability	Optional	180	7.1.5.	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made	PCP-1

					available.	
Usability	Optional	181	7.1.6.	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for an invalid credential.	Will not be tested pending availability of new ICAM Test Cards and ICAM Test PKI. Products certified prior to availability of test cards and PKI shall come into conformance within six months from the date the test cards and PKI are made available.	PCP-1
			7.2.	**Security Boundaries**		
Security	Required	182	7.2.1.	...all security relevant processing shall be performed inside the secure perimeter. No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.	Confirm all PACS components (except for the reader and the bearer's credential) are capable of being located on the secure side of perimeter. Confirm with protocol sniffing between secure/attack side	PPE-1

Security	Optional	183	7.2.2.	...compensating controls applied such as tamper switches and FIPS 140-2 certified cryptographic processing within the reader itself.	Specific waivers to 7.2.1 shall be granted on a per implementation basis of compensating controls. Document all supplemental security devices and check against APLs, FIPS 140-2. Confirm controls are operational through physical inspection, design documentation. Confirm with protocol sniffing between secure/attack side.	PPE-1
			7.3.	**Registering Physical Access Privileges**		
Usability	Optional	184	7.3.1.	Shall be able to define populations (validities) such as "guest, visitor, regular access".	Confirm physical inspection and design documentation.	PPL-4
Usability	Optional	185	7.3.2.	shall be able to define: Access points for each population	Verify by system design review	PPL-5, PAC-1
Usability	Optional	186	7.3.3.	shall be able to define: Temporal access rules for each population	Verify by system design review	PPL-5, PAC-1
Usability	Optional	187	7.3.4.	shall be able to define: Authentication mode required to support 4.2.2 and 4.2.3	Verify by system design review	PPL-5, PAC-1
Security	Required	188	7.3.5.	No credential shall be individually registered for which there is no valid trust path per the relying party PKI policy.	Derive from the overall results of testing in Section 2.	PIA-9

Security	Required	189	7.3.6.	No credential shall be individually registered where the binding of the credential to the bearer does not meet relying party security policy.	Derive from the overall results of testing in Section 2.	PIA-9
Security	Required	190	7.3.7.	No credential shall be individually authorized for access that does not meet relying party security policy.	Derive from the overall results of testing in Section 2.	PIA-9
			7.4.	**PKI Configuration**		
Security	Optional	191	7.4.1.	The solution shall provide the means to select which X.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of X.509 constraints and policies.	PIA-5
Security	Required	192	7.4.2.	The solution shall provide the means to select and manage Trust Anchors. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of trust anchors.	PSC-2
Security	Optional	193	7.4.3.	The solution may provide configuration options to ignore PKI faults in certificates (end-entity up to trust anchor). This configuration will reflect the customer’s PKI relying party policy.	Perform design review of vendor’s PKI configuration options. If options are presented to ignore PKI faults, testing shall proceed to 7.4.4.	
Security	Required	194	7.4.4.	For every event where a PKI fault is identified, the solution shall check configuration options to ignore the	Configure system to ignore PKI faults one by one, per capability of solution. Re-run appropriate	

				identified fault. If configuration allows the solution to ignore the fault, the solution shall ignore the fault and produce a warning in the audit log and store the certificate in a certificate store of failed certificates. The audit log shall indicate what failed and provide sufficient information to link the log entry to the stored certificate.	ICAM card and PKI tests for both time of registration and time of access with the appropriate fault. Inspect logs and the linked certificate store. Confirm failure is properly identified and certificate matches log entry.	
Security	Required	195	7.4.5.	If PKI faults are allowed, the solution shall provide a means to generate a report and consolidate failed certificates for transmission to appropriate parties by email. Running the report and sending the email shall be per the customer's PKI relying party policy.	Confirm ability to generate report and certificates to be sent by email.	
Security	Required	196	7.4.6.	The system shall check that the issuing certificate authority has not placed the certificate on its certificate revocation list (CRL) within the previous 6 hours.	Confirm solution's ability to set CRLs and OCSP response caching to 6 hours or less.	
			7.5.	**Credential number specifications**		
Security	Required	197	7.5.1.	The solution shall support FICAM conformant 128-bit FASC-N credential numbers as specified in *Table 3* for Time of Registration, Time of Access, and Automated Provisioning.	Configure system for 128-bit FASC-N. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate	PAU-2, PAU-3; Table 6-1 row 3

					fields, the details shall be provided to the GSA ICAM Lab for testing purposes.	
Security	Required	198	7.5.2.	The solution shall support FICAM conformant 128-bit UUID credential numbers as specified in *Table 3* for Time of Registration, Time of Access, and Automated Provisioning.	Configure system for 128-bit UUID. Review transactional test logs for registration and access. Confirm all operational usage is 128-bit and not parsed into separate fields. If the system parses the numbers into separate fields, the details shall be provided to the GSA ICAM Lab for testing purposes.	PAU-2, PAU-3; Table 6-1 row 3
Security	Required	199	7.5.3.	Systems that reduce credential numbers defined in *Table 3* to less than 128-bits within any element of the E-PACS solution shall provide compensating controls to avoid credential number collisions. The method shall achieve credential numbers that are greater than or equal to 64-bits. Compensating controls will be deprecated on 10/21/2014.	Perform design review of vendor's compensating controls. Analyze compensating controls to confirm effective credential numbers are greater than or equal to 64-bits.	PAU-2, PAU-3; Table 6-1 row 3 derived
Usability	Optional	200	7.5.4.	For 48-bit binary FASC-N ID, the solution shall be configurable to support FICAM conformant credential numbers as specified in *Table 4* for Time of Registration, Time of Access, and Automated Provisioning. This format	Configure system for 48-bit FASC-N ID. Review transactional test logs for registration and access.	PAU-2, PAU-3; Table 6-1 row 3

				will be deprecated on 10/21/2014.		
Usability	Optional	201	7.5.5.	For 64-bit FASC-N ID + CS + ICI, the solution shall be configurable to support FICAM conformant credential numbers as specified in *Table 4* for Time of Registration, Time of Access, and Automated Provisioning. This format will be deprecated on 10/21/2014.	Configure system for 64-bit FASC-N ID + CS + ICI. Review transactional test logs for registration and access.	PAU-2, PAU-3; Table 6-1 row 3
Usability	Optional	202	7.5.6.	For 200-bit Full FASC-N, the solution shall be configurable to support FICAM conformant credential numbers as specified in *Table 4* for Time of Registration, Time of Access, and Automated Provisioning. This format will be deprecated on 10/21/2014.	Configure system for 200-bit Full FASC-N. Review transactional test logs for registration and access.	PAU-2, PAU-3; Table 6-1 row 3
Security	Required	203	7.5.7.	Systems that use legacy/transitional state FASC-N credential numbers defined in *Table 4* shall provide compensating controls to avoid credential number collisions. The method shall achieve credential numbers that are greater than or equal to 64-bits. Compensating controls will be deprecated on 10/21/2014.	Perform design review of vendor's compensating controls. Analyze compensating controls to confirm effective credential numbers are greater than or equal to 64-bits.	PAU-2, PAU-3; Table 6-1 row 3 derived
			7.6.	**Validation at Time of Access**		

Usability	Optional	204	7.6.1.	Shall support Signed CHUID	Deprecated.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	205	7.6.2.	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Interface Chip card	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	206	7.6.3.	Shall support BIO	Use Authentication Test logs to verify that all good cards with valid BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	207	7.6.4.	Shall support PIV Authentication Key + PIN (PKI-AUTH)	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	208	7.6.5.	Shall support PIV Authentication Key + PIN + BIO (PKI-AUTH+BIO)	Use Authentication Test logs to verify that all good cards with valid PKI-AUTH and BIO available were allowed access at	PIA-2, PIA-3.x, PIA-4, PIA-5,

					the door reader.	PIA-6, PIA-7
Usability	Optional	209	7.6.6.	Shall support Card Authentication Key + PIN + BIO (PKI-CAK+BIO)	Use Authentication Test logs to verify that all good cards with valid PKI-CAK and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	210	7.6.7.	Shall support PKI-CAK + BIO to PACS	Use Authentication Test logs to verify that all good cards with valid BIO were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3
Usability	Optional	211	7.6.8.	Shall support PKI-AUTH + BIO to PACS	Use Authentication Test logs to verify that all good cards with valid BIO were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3
Usability	Optional	212	7.6.9.	Shall support contact Card Authentication Key (PKI-CAK) for Dual Interface Chip card	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5,

						PIA-6, PIA-7
Usability	Optional	213	7.6.10.	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Chip card	Requirements for Dual Chip Cards will not be tested prior to June 1, 2014. These requirements become mandatory as of June 1, 2014. Products certified prior to June 1, 2014 shall come into conformance within six months from the date the test cards and PKI are made available for dual chip testing.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Security	Required	214	7.6.11.	E-PACS portal solutions shall not support legacy technologies when configured for approved FICAM modes.	Verify solution turns off legacy modes when an approved FICAM mode is enabled. With reader set to PKI-AUTH, attempt to use 125KHz, DESFire, iClass, Indala and related legacy technologies. All access attempts with legacy shall be denied.	
			7.7.	**Portal Hardware**		
Security	Required	215	7.7.1.	Product shall support Reader to PACS communications using bi-directional technology. This includes a minimum of one of RS-485, Ethernet, secure wireless.	Verify by system design review. Confirmed using protocol sniffing, review of logs produced during authentication testing.	PCM-2, PCM-3

Usability	Optional	216	7.7.2.	For multi-factor readers, applicant's system must allow an administrator to modify an individual reader's authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	217	7.7.3.	For multi-factor readers, applicant's system must allow an administrator to modify a group of readers' authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	218	7.7.4.	For multi-factor readers, the site administrator shall not be required to approach and touch each reader to change its authentication mode (authentication factors).	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	219	7.7.5.	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	220	7.7.6.	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) on a time based	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to	PCM-3

				schedule.	mode.	
Usability	Optional	221	7.7.7.	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	222	7.7.8.	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Required	223	7.7.9.	Contact readers shall support ISO/IEC 7816.	The contact interface of the reader shall be tested for ISO/IEC 7816 conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-3:2010 Sections 4, 7, and 8. Vendor shall provide a test data report documenting conformance for review and	[FIPS 201]

					approval.	
Usability	Required	224	7.7.10.	Contactless readers shall support ISO/IEC 14443 Type A.	The contactless interface of the reader shall be tested for ISO/IEC 14443 Type A conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-6:2011 Sections 4, 5, 6.1, 7.1 and 8.1, and ISO/IEC 10373-6:2011/Amd.4:2012. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]
Security	Required	225	7.7.11.	ISO/IEC 14443 Type A contactless readers shall not activate and operate with a PIV card beyond 10cm.	Card 1 is presented at 11cm to the reader. All contactless PIV authentication modes shall fail.	[FIPS 201]
Usability	Required	226	7.7.12.	ISO/IEC 14443 Type A contactless readers shall provide sufficient field strength to activate and operate with a PIV card at or below 3.5cm.	Card 1 is presented at 3.5cm to the reader. All contactless PIV authentication modes shall succeed.	[FIPS 201]
Security	Optional	227	7.7.13.	The System shall protect the communications between readers and the PACS using a cryptographically	FICAM profile for OSDP to be developed in next spiral of	PSC-1

				secure protocol.	FICAM Testing Program.	
Usability	Optional	228	7.7.14.	For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes, this too shall be considered non-compliant.	Verify by system design review	PCM-3
			7.8.	**Auditing and Logging**		
Security	Required	229	7.8.1.	Granularity of auditing records shall be to the card and individual transaction. These shall be easily verifiable through a reporting tool or any other log and audit viewing capability	Verify by review of logs and reports	PAU-1, PAU-2, PAU-7
Security	Required	230	7.8.2.	The product shall provide auditing/logging of all PKI processing to include - Pass/fail from a Challenge/Response - PDVAL - Disabling credential based on PDVAL, expiration or revocation status	Verify by review of logs and reports; confirmed by protocol sniffing	PAU-3, PAU-4, PAU-7
Security	Required	231	7.8.3.	The product shall provide auditing/logging of credential number processing and transmission	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7
Security	Required	232	7.8.4.	The product shall provide auditing/logging of all software driven configuration changes	Verify by review of logs and reports	PAU-6, PAU-7

Security	Required	233	7.8.5.	The product shall provide auditing/logging of periodic certificate PDVAL and status checking	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7
Security	Required	234	7.8.6.	The product shall provide auditing/logging of Card activity (e.g., 3 days of card activity)	Verify by review of logs and reports	PAU-3, PAU-7
Security	Required	235	7.8.7.	The product shall provide auditing/logging of last known location of a card in system	Verify by review of logs and reports	PAU-3, PAU-7
Security	Required	236	7.8.8.	The product shall provide auditing/logging of PKI policies for name constraints, path constraints, validity checks	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7
Security	Required	237	7.8.9.	The product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop)	Verify by review of logs and reports	PAU-3, PAU-7
Security	Required	238	7.8.10.	The product shall provide auditing/logging of what date individuals were provisioned or de-provisioned and by whom	Verify by review of logs and reports	PAU-4, PAU-7
Security	Required	239	7.8.11.	The product shall provide auditing/logging of all readers and their modes	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7
Security	Required	240	7.8.12.	The product shall provide auditing/logging of configuration	Verify by review of logs and	PAU-5, PAU-6,

				download status to system components	reports	PAU-7
			7.9.	**Security Certification and Accreditation**		
Usability	Required	241	7.9.1.	As required by UL 294, relevant components within the solution shall have a UL 294 listing	Verify UL listing. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-2
Usability	Required	242	7.9.2.	As required by UL 1076, relevant components within the solution shall have a UL 1076 listing	Verify UL listing. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-2 derived
Usability	Required	243	7.9.3.	As required by UL 1981, relevant components within the solution shall have a UL 1981 listing	Verify UL listing. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-2 derived
Usability	Required	244	7.9.4.	When adding a component to an existing system under a given topology, each existing component in the existing system under that topology shall have GSA FIPS-201-1 APL status.	Verify APL listing. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-3
Security	Required	245	7.9.5.	Each component leveraging cryptography in the system shall have FIPS 140-2 certification.	Verify NIST CMVP listing. Must be applied for and in process for certification before any testing can be done. Must be listed before final testing and certification by	PCA-4

					GSA FIPS 201 APL program.	
			7.10.	**Biometric in PACS**		
Security	Optional	246	7.10.1.	Shall follow PIA-3.4 Detailed Guidance Case 3 for biometric identifiers leveraged in BIO to PACS.	Verify by system design and inspection of database	PIA-3.4
			7.11.	**Operational Controls**		
Security	Required	247	7.11.1.	The system shall have the ability to enforce administrative privilege for configuration management operations.	Verify by use of the system.	PCM-1
Security	Required	248	7.11.2.	Shall authenticate administrators using a process of equivalent or greater assurance than the authentication modes supported by the system. This may be done using E-Auth LOA-4 credentials.	Verify by use of the system.	PCM-1
Usability	Optional	249	7.11.3.	The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree	Verify by use of the system.	PCM-2

Usability	Optional	250	7.11.4.	Each physical component shall be separately defined and addressable within the server user interface	Verify by setting up of system.	PCM-2
Usability	Optional	251	7.11.5.	The system shall support configuration downloads to relevant components	Verify by setting up of system.	PCM-2